REMARKS

The Examiner has rejected Claims 1-3, 7-12, 16-21, and 25-27 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No.: 5,557,742 to Smaha et al., in view of U.S. Patent No.: 5,513,317 to Borchardt et al. Applicant respectfully disagrees with such rejection.

It appears that the Examiner continues to rely on Smaha to make a prior art showing of applicant's claimed:

"receiving an audit specification;

wherein the audit specification specifies at least one target attribute to be recorded from a set of possible target attributes during an auditing process by the auditing system;

wherein the audit specification also specifies at least one auditing criterion that triggers recording of the at least one target attribute during the auditing process;

configuring the auditing system to record the at least one target attribute in response to detecting the at least one auditing criterion."

Specifically, the Examiner has now equated applicant's claimed "audit specification" to Smaha's "selected misuses," wherein a misuse is a "target attribute."

This is simply incorrect. Applicant's claimed "audit specification" is not a misuse, but rather a specification that is used to configure an auditing system for creating an audit log that is, in turn, examined to detect patterns for intrusion detection purposes. Thus, it is applicant's claimed "patterns" that are most analogous to Smaha's "selected misuses" and associated signature data structures, not applicant's claimed "audit specification."

It appears that the Examiner is attempting to arbitrarily map various terms in applicant's claims with those in the Smaha reference. Specifically, it appears that the Examiner is relying on Smaha's "selected misuses" (and associated signatures) to meet both applicant's claimed "audit specification" and "patterns." However, such attempt clearly fails, since the remaining functionality of applicant's claim is simply not met. For example, simply nowhere in Smaha are the "selected

misuses" (which is allegedly equivalent to applicant's claimed "audit specification," per the Examiner) used to configure an audit system to produce an audit log which is, in turn, "examin[ed] ... to detect patterns for intrusion detection purposes." While Smaha's "selected misuses" may be used to detect patterns for intrusion detection purposes, they are simply *not* used to configure an audit system to produce an audit log for recording purposes, as claimed. It appears that the Examiner is improperly attempting to use a single entity (i.e. "selected misuses") in Smaha to meet two entities (i.e. "audit specification" and "patterns") in applicant's claims. This obviously fails, especially since the related functionality is not met by Smaha.

Again, the primary reason that Smaha fails is due to the fact that it does not disclose the crux of applicant's claimed invention that is embodied in the claims, nor the problem that it solves. As indicated on page 11, first paragraph of the originally file specification: by selectively recording target attributes, the present invention can reduce the amount of data that is recorded during the auditing process. This makes it practical to record data that is read or written during system calls without overwhelming the storage capacity, processing power and/or data transfer bandwidth of a computer system.

Applicant's claimed invention thus limits the amount of data that is even subjected to pattern (i.e. "misuse, etc.) detection.

The Examiner now continues by relying on the following excerpt from Borchardt et al. to make a prior art showing of applicant's claimed "size of the audit log [being] reduced when the auditing system is run prior to the examination for detection of the patterns."

> "First, the program is executed while the trace facility is active (Step 104). However, rather than immediately supply text representation of the filtered entries to the programmer, the trace facility gathers all historical trace data which may be pertinent to any category/filter of the trace criteria (Step 106). Trace output categories are defined which map to the filtering criteria, and each trace output entry which is produced during execution is associated with one or more of these categories. This data is stored in memory 10 for future use (Step 108). Accordingly, all of the information generated by the trace facility remains available to the user. These trace entries retain information regarding their origin, and thus remain usable, as opposed to the filtered text which is output by the prior art and may only be further filtered with regard to text strings

> found in the different entries, if at all. The trace entries may be stored in many forms, but it has been found that storing them as object oriented objects is preferable, since the nature of such objects lends itself to maintaining the identity or origin information of the data produced by the trace facility." (col. 4, lines 1-19)

Moreover, the Examiner argues that it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the system disclosed by Smaha by filtering according to one or more attributes before analysis. Applicant respectfully disagrees with this assertion of "obviousness," especially in view of ample evidence to the contrary.

For example, Smaha relates to an intrusion detection system, while Borchardt relates to a software debugger. To simply glean features from a software bugger, such as that of Borchardt, and combine the same with the *non-analogous art* of intrusion detection systems, such as that of Smaha, would simply be improper. Software debuggers detect code problems in newly created software, while an intrusion detection system detects hacker activity. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a software bugger addresses as opposed to an intrusion detection system, the Examiner's proposed combination is inappropriate.

More importantly, the foregoing excerpt and the remaining portions of the Borchardt reference, fails to disclose, teach or suggest any sort of "size of the audit log [being] reduced when the auditing system is run prior to the examination for detection of the patterns" (emphasis added). Instead, Borchardt simply discloses the detection of "inadvertent programming errors," or "bugs." This is vastly different from the "patterns" used for "intrusion detection purposes," as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, for the reasons set forth hereinabove.

All of the independent claims are thus deemed allowable for the reasons set forth hereinabove. Moreover, by virtue of their dependence on such claims, all of the remaining dependent claims are also deemed allowable.

A notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P250).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100